



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/684,400	10/15/2003	Motoji Ohmori	2003_1474A	4423
513 7590 01/22/2008 WENDEROTH, LIND & PONACK, L.L.P. 2033 K STREET N. W. SUITE 800 WASHINGTON, DC 20006-1021			EXAMINER AVERY, JEREMIAH L	
			ART UNIT 2131	PAPER NUMBER
			MAIL DATE 01/22/2008	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

CG

Office Action Summary	Application No. 10/684,400	Applicant(s) OHMORI ET AL.	
	Examiner Jeremiah Avery	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 19 December 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 19-33 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 19-33 is/are rejected.
- 7) ☒ Claim(s) 19,22,26,27,30,32 and 33 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 15 October 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) ☒ Notice of References Cited (PTO-892) | 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) ☐ Notice of Informal Patent Application |
| 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) ☐ Other: _____ |

DETAILED ACTION

1. Claims 19-33 have been examined.
2. Responses to Applicant's remarks have been given.

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 12/19/07 has been entered.

Claim Objections

2. Claims 19, 22, 26, 27, 30, 32 and 33 are objected to because of the following informalities: usage of the term "operable". It has been held that the recitation that an element being "operable to" perform a function is not a positive limitation but only requires the ability to so perform. It does not constitute a limitation in any patentable sense. Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 19-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over United States Patent No. 6,820,204 to Desai et al., hereinafter Desai and further in view of United States Patent No. 6,061,799 to Eldridge et al., hereinafter Eldridge.

3. Desai significantly discloses the claimed invention as cited below, however fails to fully disclose each limitation. Eldridge discloses these limitations, as cited below.

4. Regarding claim 19, Desai and Eldridge disclose a password recovery system for re-supplying a password to a user who has forgotten the password, said password recovery system comprising:

a communication terminal device (*Desai* – column 2, lines 29-53, column 3, lines 42-62 and column 8, lines 27-41);

a portable password recording medium having the password recorded thereon and being coupled to said communication terminal device (*Desai* – Figure 11, column 2, lines 29-53, column 3, lines 42-62, column 5, lines 66 and 67, column 6, lines 1-25, column 9, lines 1-18, “registered user’s profile data is kept private by the information exchange system 10 until the registered user 12 provides access to a view of the stored data”, column 15, lines 27-44 and 55-67 and column 16, lines 1-3 and *Eldridge* – column 8, lines 63-67, column 9, lines 1-13 and 28-35 and column 11, lines 5-33, “diskette 142, CD-ROM 147”),

wherein said communication terminal device comprises:

a first receiving unite operable to receive, from an external communication terminal device, a signed data set generated with use of a secret key belonging to a guarantor who guarantees legitimacy of the user (*Desai* – Figure 6, column 8, lines 27-41, column 10, lines 7-19, column 12, lines 29-41 and 54-67, column 13, lines 1-8, column 14, lines 35-55, column 15, lines 27-44, column 16, lines 34-42, column 17, lines 11-40 and column 21, lines 10-30 and *Eldridge* – Figures 3A, 3B, 5, 6B and 9, column 1, lines 66 and 67, column 2, lines 1-8, 31-47 and 64-67, column 3, lines 1-10, column 4, lines 62-67, column 5, lines 1-24, “one type of encryption key suitable for use as secret parameter 302 is a RSA private encryption key”, column 7, lines 19-48, column 8, lines 63-67 and column 9, lines 1-13 and 28-35);

an outputting unit operable to output the signed data set received by said first receiving unit to said password recording medium (*Desai* – column 4, lines 32-67, “information exchange system and its storage system may be distributed across a

plurality of devices”, column 5, lines 66 and 67, column 6, lines 1-25, column 9, lines 19-31, column 15, lines 27-44 and 55-67, column 16, lines 1-3, column 20, lines 36-67, column 21, lines 1-9 and column 22, lines 23-43),
wherein said password recording medium comprises:

a public key storing unit for storing therein a public key that corresponds to the secret key (*Desai* – column 5, lines 24-39, column 12, lines 29-41 and 54-67, column 13, lines 1-8, column 15, lines 27-67, column 16, lines 1-3 and 34-42, column 17, lines 11-40 and column 21, lines 10-30);

a password storing unit for storing the password therein (*Desai* – Figure 11, column 2, lines 29-53, column 3, lines 42-62, column 5, lines 66 and 67, column 6, lines 1-25, column 9, lines 1-18, “registered user’s profile data is kept private by the information exchange system 10 until the registered user 12 provides access to a view of the stored data”, column 15, lines 27-44 and 55-67 and column 16, lines 1-3);

a second receiving unit operable to receive the signed data set output by said outputting unit (*Desai* – column 4, lines 32-67, “information exchange system and its storage system may be distributed across a plurality of devices”, column 5, lines 66 and 67, column 6, lines 1-25, column 9, lines 19-31, column 15, lines 27-44 and 55-67, column 16, lines 1-3, column 20, lines 36-67, column 21, lines 1-9 and column 22, lines 23-43);

an authentication unit operable to read the public key from said public key storing unit and perform signature authentication using the read public key and the signed data set received by said second receiving unit to judge whether the signed data set received

by said second receiving unit has been signed by the guarantor (*Desai* – Figures 11 and 17, column 2, lines 29-53, column 3, lines 42-62, column 5, lines 66 and 67, column 6, lines 1-25, column 9, lines 1-18, “registered user's profile data is kept private by the information exchange system 10 until the registered user 12 provides access to a view of the stored data”, column 15, lines 27-44 and 55-67, column 16, lines 1-3 and column 18, lines 53-67 and *Eldridge* – Figures 3A, 3B, 5, 6B and 9, column 1, lines 66 and 67, column 2, lines 1-8, 31-47 and 64-67, column 3, lines 1-10, column 4, lines 62-67, column 5, lines 1-24, “one type of encryption key suitable for use as secret parameter 302 is a RSA private encryption key”, column 7, lines 19-48, column 8, lines 63-67 and column 9, lines 1-13 and 28-35);

a reading unit operable, when said authentication unit judges that said data set received by said second receiving unit has been signed by the guarantor, to read the password from said password storing unit (*Desai* – Figures 11 and 17, column 9, lines 1-18, “registered user's profile data is kept private by the information exchange system 10 until the registered user 12 provides access to a view of the stored data”, column 18, lines 53-67, column 20, lines 36-67, column 21, lines 1-9 and column 22, lines 23-43 and *Eldridge* – Figures 3A, 3B, 5, 6B and 9, column 1, lines 66 and 67, column 2, lines 1-8, 31-47 and 64-67, column 3, lines 1-10, column 4, lines 62-67, column 5, lines 1-24, “one type of encryption key suitable for use as secret parameter 302 is a RSA private encryption key”, column 7, lines 19-48, column 8, lines 63-67 and column 9, lines 1-13 and 28-35).

5. Regarding claim 20, Desai and Eldridge disclose wherein said password recording medium further comprises an expiration period storing unit for storing therein an expiration period for receiving the signed data set (*Desai* – column 13, lines 39-52), wherein the signed data set received by said second receiving unit has date/time information attached thereto, the data/time information indicating a date and time at which the signed data set has been generated (*Desai* – column 31, lines 5-24), wherein said authentication unit performs the signature authentication so as to judge if the signed data set received by said second receiving unit has been signed by the guarantor, and judges if the date/time information attached to the signed data set is within the expiration period stored in said expiration period storing unit (*Desai* – Figures 11 and 17, column 2, lines 29-53, column 3, lines 42-62, column 5, lines 66 and 67, column 6, lines 1-25, column 9, lines 1-18, “registered user’s profile data is kept private by the information exchange system 10 until the registered user 12 provides access to a view of the stored data”, column 13, lines 39-52, column 15, lines 27-44 and 55-67, column 16, lines 1-3 and column 18, lines 53-67 and *Eldridge* – Figures 3A, 3B, 5, 6B and 9, column 1, lines 66 and 67, column 2, lines 1-8, 31-47 and 64-67, column 3, lines 1-10, column 4, lines 62-67, column 5, lines 1-24, “one type of encryption key suitable for use as secret parameter 302 is a RSA private encryption key”, column 7, lines 19-48, column 8, lines 63-67 and column 9, lines 1-13 and 28-35), wherein said reading unit reads the password from said password storing unit if said authentication unit judges that the received signed data set has been signed by the guarantor and that the date/time information is within the expiration period (*Desai* –

Figures 11 and 17, column 9, lines 1-18, "registered user's profile data is kept private by the information exchange system 10 until the registered user 12 provides access to a view of the stored data", column 13, lines 39-52, column 18, lines 53-67, column 20, lines 36-67, column 21, lines 1-9 and column 22, lines 23-43 and *Eldridge* – Figures 3A, 3B, 5, 6B and 9, column 1, lines 66 and 67, column 2, lines 1-8, 31-47 and 64-67, column 3, lines 1-10, column 4, lines 62-67, column 5, lines 1-24, "one type of encryption key suitable for use as secret parameter 302 is a RSA private encryption key", column 7, lines 19-48, column 8, lines 63-67 and column 9, lines 1-13 and 28-35).

6. Regarding claim 21, Desai and Eldridge disclose wherein said password recording medium further comprises a signed data set number storing unit for storing therein a predetermined number indicating an amount of signed data sets that are required for performing a password recovery (*Desai* – Figure 11, column 2, lines 29-53, column 3, lines 42-62, column 5, lines 66 and 67, column 6, lines 1-25, column 9, lines 1-18, "registered user's profile data is kept private by the information exchange system 10 until the registered user 12 provides access to a view of the stored data", column 15, lines 27-44 and 55-67 and column 16, lines 1-3), wherein said reading unit counts the received signed data set as a valid signed data set for performing the password recovery when said authentication unit judges that the signed data set received by said second receiving unit has been signed by the guarantor, and reads the password from said password storing unit when the amount of valid signed data sets has reached the predetermined number stored in said signed data set number storing unit (*Desai* – Figure 11, column 2, lines 29-53, column 3, lines

42-62, column 5, lines 66 and 67, column 6, lines 1-25, column 9, lines 1-18, "registered user's profile data is kept private by the information exchange system 10 until the registered user 12 provides access to a view of the stored data", column 15, lines 27-67 and column 16, lines 1-3 and *Eldridge* – Figures 3A, 3B, 5, 6B and 9, column 1, lines 66 and 67, column 2, lines 1-8, 31-47 and 64-67, column 3, lines 1-10, column 4, lines 62-67, column 5, lines 1-24, "one type of encryption key suitable for use as secret parameter 302 is a RSA private encryption key", column 7, lines 19-48, column 8, lines 63-67 and column 9, lines 1-13 and 28-35).

7. Regarding claim 22, Desai and Eldridge disclose a communication terminal device for re-supplying a password to a user who has forgotten the password (*Desai* – column 15, lines 27-67 and column 16, lines 1-3),

said communication terminal comprising:

a public key storing unit for storing therein a public key that corresponds to a secret key belonging to a guarantor who guarantees legitimacy of the user (*Desai* – column 5, lines 24-39, column 12, lines 29-41 and 54-67, column 13, lines 1-8, column 15, lines 27-67, column 16, lines 1-3 and 34-42, column 17, lines 11-40 and column 21, lines 10-30 and *Eldridge* – Figures 3A, 3B, 5, 6B and 9, column 1, lines 66 and 67, column 2, lines 1-8, 31-47 and 64-67, column 3, lines 1-10, column 4, lines 62-67, column 5, lines 1-24, "one type of encryption key suitable for use as secret parameter 302 is a RSA private encryption key", column 7, lines 19-48, column 8, lines 63-67 and column 9, lines 1-13 and 28-35);

a password storing unit for storing the password therein (*Desai* – Figure 11, column 2, lines 29-53, column 3, lines 42-62, column 5, lines 66 and 67, column 6, lines 1-25, column 9, lines 1-18, “registered user’s profile data is kept private by the information exchange system 10 until the registered user 12 provides access to a view of the stored data”, column 15, lines 27-44 and 55-67 and column 16, lines 1-3);

a receiving unit operable to receive, from an external communication terminal device, a signed data set generated with use of the secret key (*Desai* – column 4, lines 32-67, “information exchange system and its storage system may be distributed across a plurality of devices”, column 5, lines 66 and 67, column 6, lines 1-25, column 9, lines 19-31, column 15, lines 27-44 and 55-67, column 16, lines 1-3, column 20, lines 36-67, column 21, lines 1-9 and column 22, lines 23-43);

an authentication unit operable to read the public key from said public key storing unit and perform signature authentication using the read public key and the signed data set received by said receiving unit to judge whether the signed data set received by said receiving unit has been signed by the guarantor (*Desai* – Figures 11 and 17, column 2, lines 29-53, column 3, lines 42-62, column 5, lines 66 and 67, column 6, lines 1-25, column 9, lines 1-18, “registered user’s profile data is kept private by the information exchange system 10 until the registered user 12 provides access to a view of the stored data”, column 15, lines 27-44 and 55-67, column 16, lines 1-3 and column 18, lines 53-67 and *Eldridge* – Figures 3A, 3B, 5, 6B and 9, column 1, lines 66 and 67, column 2, lines 1-8, 31-47 and 64-67, column 3, lines 1-10, column 4, lines 62-67, column 5, lines 1-24, “one type of encryption key suitable for use as secret parameter 302 is a RSA

private encryption key”, column 7, lines 19-48, column 8, lines 63-67 and column 9, lines 1-13 and 28-35);

a reading unit operable, when said authentication unit judges that the signed data set received by said receiving unit has been signed by the guarantor, to read the password from said password storing unit (*Desai* – Figures 11 and 17, column 9, lines 1-18, “registered user’s profile data is kept private by the information exchange system 10 until the registered user 12 provides access to a view of the stored data”, column 18, lines 53-67, column 20, lines 36-67, column 21, lines 1-9 and column 22, lines 23-43 and *Eldridge* – Figures 3A, 3B, 5, 6B and 9, column 1, lines 66 and 67, column 2, lines 1-8, 31-47 and 64-67, column 3, lines 1-10, column 4, lines 62-67, column 5, lines 1-24, “one type of encryption key suitable for use as secret parameter 302 is a RSA private encryption key”, column 7, lines 19-48, column 8, lines 63-67 and column 9, lines 1-13 and 28-35).

8. Regarding claim 23, *Desai* and *Eldridge* disclose an expiration period storing unit for storing therein an expiration period for receiving the signed data set (*Desai* – column 13, lines 39-52, “access may automatically expire after the passing of a certain amount of time or a certain amount of accesses to the data element”), wherein the signed data set received by said receiving unit has date/time information attached thereto, the date/time information indicating a date and time at which the signed data set has been generated (*Desai* – column 31, lines 5-24), wherein said authentication unit performs the signature authentication so as to judge if the signed data set received by said receiving unit has been signed by the guarantor,

and judges if the date/time information attached to the signed data set is within the expiration period stored in the expiration period storing unit (*Desai* – Figures 11 and 17, column 2, lines 29-53, column 3, lines 42-62, column 5, lines 66 and 67, column 6, lines 1-25, column 9, lines 1-18, “registered user’s profile data is kept private by the information exchange system 10 until the registered user 12 provides access to a view of the stored data”, column 13, lines 39-52, column 15, lines 27-44 and 55-67, column 16, lines 1-3 and column 18, lines 53-67 and *Eldridge* – Figures 3A, 3B, 5, 6B and 9, column 1, lines 66 and 67, column 2, lines 1-8, 31-47 and 64-67, column 3, lines 1-10, column 4, lines 62-67, column 5, lines 1-24, “one type of encryption key suitable for use as secret parameter 302 is a RSA private encryption key”, column 7, lines 19-48, column 8, lines 63-67 and column 9, lines 1-13 and 28-35), wherein said reading unit reads the password from said password storing unit if said authentication unit judges that the signed data set received by said receiving unit has been signed by the guarantor and that the date/time information is within the expiration period (*Desai* – Figures 11 and 17, column 9, lines 1-18, “registered user’s profile data is kept private by the information exchange system 10 until the registered user 12 provides access to a view of the stored data”, column 13, lines 39-52, column 18, lines 53-67, column 20, lines 36-67, column 21, lines 1-9 and column 22, lines 23-43 and *Eldridge* – Figures 3A, 3B, 5, 6B and 9, column 1, lines 66 and 67, column 2, lines 1-8, 31-47 and 64-67, column 3, lines 1-10, column 4, lines 62-67, column 5, lines 1-24, “one type of encryption key suitable for use as secret parameter 302 is a RSA private

encryption key", column 7, lines 19-48, column 8, lines 63-67 and column 9, lines 1-13 and 28-35).

9. Regarding claim 24, Desai and Eldridge disclose a signed data set number storing unit for storing therein a predetermined number indicating an amount of signed data sets that are required for performing a password recovery (*Desai* – Figure 11, column 2, lines 29-53, column 3, lines 42-62, column 5, lines 66 and 67, column 6, lines 1-25, column 9, lines 1-18, "registered user's profile data is kept private by the information exchange system 10 until the registered user 12 provides access to a view of the stored data", column 15, lines 27-44 and 55-67 and column 16, lines 1-3), wherein said reading unit counts the received signed data set as a valid signed data set for performing the password recovery when said authentication unit judges that the received signed data set has been signed by the guarantor, and reads the password from said password storing unit when the amount of valid signed data sets has reached the predetermined number stored in said signed data set number storing unit (*Desai* – Figure 11, column 2, lines 29-53, column 3, lines 42-62, column 5, lines 66 and 67, column 6, lines 1-25, column 9, lines 1-18, "registered user's profile data is kept private by the information exchange system 10 until the registered user 12 provides access to a view of the stored data", column 15, lines 27-67 and column 16, lines 1-3 and *Eldridge* – Figures 3A, 3B, 5, 6B and 9, column 1, lines 66 and 67, column 2, lines 1-8, 31-47 and 64-67, column 3, lines 1-10, column 4, lines 62-67, column 5, lines 1-24, "one type of encryption key suitable for use as secret parameter 302 is a RSA private encryption key", column 7, lines 19-48, column 8, lines 63-67 and column 9, lines 1-13 and 28-35).

10. Regarding claim 25, Desai discloses a displaying unit operable to display the password read by said reading unit (column 4, lines 32-67, "information exchange system and its storage system may be distributed across a plurality of devices", column 5, lines 66 and 67, column 6, lines 1-25, column 9, lines 19-31, column 15, lines 27-44 and 55-67, column 16, lines 1-3, column 20, lines 36-67, column 21, lines 1-9 and column 22, lines 23-43).

11. Regarding claim 26, Desai discloses an application storing unit for storing therein a piece of application software that corresponds to the password (column 1, lines 26-51, column 2, lines 3-53, column 3, lines 42-67, column 4, lines 1-31, column 9, lines 1-18, "registered user's profile data is kept private by the information exchange system 10 until the registered user 12 provides access to a view of the stored data", column 15, lines 27-44 and 55-67 and column 16, lines 1-3);

an application executing unit operable to execute the pieces of application software, using the password read by said reading unit (column 1, lines 26-51, column 2, lines 3-53, column 3, lines 42-67, column 4, lines 1-31, column 9, lines 1-18, "registered user's profile data is kept private by the information exchange system 10 until the registered user 12 provides access to a view of the stored data", column 15, lines 27-44 and 55-67 and column 16, lines 1-3).

12. Regarding claim 27, Desai and Eldridge disclose a password recording medium that is portable and operable to re-supply a password to a user who has forgotten the password (*Desai* – column 2, lines 29-53, column 3, lines 42-62, column 8, lines 27-41, column 15, lines 27-67 and column 16, lines 1-3 and *Eldridge* – column 8, lines 63-67,

column 9, lines 1-13 and 28-35 and column 11, lines 5-33, "diskette 142, CD-ROM 147"),

said password recording medium comprising:

a public key storing unit for storing therein a public key that corresponds to a secret key belonging to a guarantor who guarantees legitimacy of the user (*Desai* – column 5, lines 24-39, column 12, lines 29-41 and 54-67, column 13, lines 1-8, column 15, lines 27-67, column 16, lines 1-3 and 34-42, column 17, lines 11-40 and column 21, lines 10-30 and *Eldridge* – Figures 3A, 3B, 5, 6B and 9, column 1, lines 66 and 67, column 2, lines 1-8, 31-47 and 64-67, column 3, lines 1-10, column 4, lines 62-67, column 5, lines 1-24, "one type of encryption key suitable for use as secret parameter 302 is a RSA private encryption key", column 7, lines 19-48, column 8, lines 63-67 and column 9, lines 1-13 and 28-35);

a password storing unit for storing the password therein (*Desai* – Figure 11, column 2, lines 29-53, column 3, lines 42-62, column 5, lines 66 and 67, column 6, lines 1-25, column 9, lines 1-18, "registered user's profile data is kept private by the information exchange system 10 until the registered user 12 provides access to a view of the stored data", column 15, lines 27-44 and 55-67 and column 16, lines 1-3);

a receiving unit operable to receive, from a communication terminal device to which said password recording medium is coupled, a signed data set generated with use of the secret key (*Desai* – column 4, lines 32-67, "information exchange system and its storage system may be distributed across a plurality of devices", column 5, lines 66 and 67, column 6, lines 1-25, column 9, lines 19-31, column 15, lines 27-44 and 55-67,

column 16, lines 1-3, column 20, lines 36-67, column 21, lines 1-9 and column 22, lines 23-43);

an authentication unit operable to read the public key from said public key storing unit and perform signature authentication using the read public key and the signed data set received by said receiving unit to judge whether the signed data set received by said receiving unit has been signed by the guarantor (*Desai* – Figures 11 and 17, column 2, lines 29-53, column 3, lines 42-62, column 5, lines 66 and 67, column 6, lines 1-25, column 9, lines 1-18, “registered user’s profile data is kept private by the information exchange system 10 until the registered user 12 provides access to a view of the stored data”, column 15, lines 27-44 and 55-67, column 16, lines 1-3 and column 18, lines 53-67 and *Eldridge* – Figures 3A, 3B, 5, 6B and 9, column 1, lines 66 and 67, column 2, lines 1-8, 31-47 and 64-67, column 3, lines 1-10, column 4, lines 62-67, column 5, lines 1-24, “one type of encryption key suitable for use as secret parameter 302 is a RSA private encryption key”, column 7, lines 19-48, column 8, lines 63-67 and column 9, lines 1-13 and 28-35);

a reading unit operable, when said authentication unit judges that the signed data set received by said receiving unit has been signed by the guarantor, to read the password from said password storing unit (*Desai* – Figures 11 and 17, column 9, lines 1-18, “registered user’s profile data is kept private by the information exchange system 10 until the registered user 12 provides access to a view of the stored data”, column 18, lines 53-67, column 20, lines 36-67, column 21, lines 1-9 and column 22, lines 23-43 and *Eldridge* – Figures 3A, 3B, 5, 6B and 9, column 1, lines 66 and 67, column 2, lines

1-8, 31-47 and 64-67, column 3, lines 1-10, column 4, lines 62-67, column 5, lines 1-24, "one type of encryption key suitable for use as secret parameter 302 is a RSA private encryption key", column 7, lines 19-48, column 8, lines 63-67 and column 9, lines 1-13 and 28-35).

13. Regarding claim 28, Desai and Eldridge disclose an expiration storing unit for storing therein an expiration period for receiving the signed data set (column 13, lines 39-52),

wherein the signed data set received by said receiving unit has data/time information attached thereto, the date/time information indicating a date and time at which the signed data set has been generated (*Desai* – column 31, lines 5-24),

wherein said authentication unit performs the signature authentication so as to judge if the signed data set received by said receiving unit has been signed by the guarantor,

and judges if the date/time information attached to the signed data set is within the expiration period stored in said expiration period storing unit (*Desai* – Figures 11 and 17, column 2, lines 29-53, column 3, lines 42-62, column 5, lines 66 and 67, column 6, lines 1-25, column 9, lines 1-18, "registered user's profile data is kept private by the information exchange system 10 until the registered user 12 provides access to a view of the stored data", column 13, lines 39-52, column 15, lines 27-44 and 55-67, column 16, lines 1-3 and column 18, lines 53-67 and *Eldridge* – Figures 3A, 3B, 5, 6B and 9, column 1, lines 66 and 67, column 2, lines 1-8, 31-47 and 64-67, column 3, lines 1-10, column 4, lines 62-67, column 5, lines 1-24, "one type of encryption key suitable for use

as secret parameter 302 is a RSA private encryption key”, column 7, lines 19-48, column 8, lines 63-67 and column 9, lines 1-13 and 28-35), wherein said reading unit reads the password from said password storing unit if said authentication unit judges that the signed data set received by said receiving unit has been signed by the guarantor and that the date/time information is within the expiration period (*Desai* – Figures 11 and 17, column 9, lines 1-18, “registered user’s profile data is kept private by the information exchange system 10 until the registered user 12 provides access to a view of the stored data”, column 13, lines 39-52, column 18, lines 53-67, column 20, lines 36-67, column 21, lines 1-9 and column 22, lines 23-43 and *Eldridge* – Figures 3A, 3B, 5, 6B and 9, column 1, lines 66 and 67, column 2, lines 1-8, 31-47 and 64-67, column 3, lines 1-10, column 4, lines 62-67, column 5, lines 1-24, “one type of encryption key suitable for use as secret parameter 302 is a RSA private encryption key”, column 7, lines 19-48, column 8, lines 63-67 and column 9, lines 1-13 and 28-35).

14. Regarding claim 29, *Desai* and *Eldridge* disclose a signed data set number storing unit for storing therein a predetermined number indicating an amount of signed data sets required for performing a password recovery (*Desai* –Figure 11, column 2, lines 29-53, column 3, lines 42-62, column 5, lines 66 and 67, column 6, lines 1-25, column 9, lines 1-18, “registered user’s profile data is kept private by the information exchange system 10 until the registered user 12 provides access to a view of the stored data”, column 15, lines 27-44 and 55-67 and column 16, lines 1-3),

wherein said reading unit counts the received signed data set as a valid signed data set for performing the password recovery when said authentication unit judges that the received signed data set has been signed by the guarantor, and reads the password from said password storing unit when the amount of valid signed data sets has reached the predetermined number stored in said signed data set number storing unit (*Desai* – Figure 11, column 2, lines 29-53, column 3, lines 42-62, column 5, lines 66 and 67, column 6, lines 1-25, column 9, lines 1-18, “registered user’s profile data is kept private by the information exchange system 10 until the registered user 12 provides access to a view of the stored data”, column 15, lines 27-67 and column 16, lines 1-3 and *Eldridge* – Figures 3A, 3B, 5, 6B and 9, column 1, lines 66 and 67, column 2, lines 1-8, 31-47 and 64-67, column 3, lines 1-10, column 4, lines 62-67, column 5, lines 1-24, “one type of encryption key suitable for use as secret parameter 302 is a RSA private encryption key”, column 7, lines 19-48, column 8, lines 63-67 and column 9, lines 1-13 and 28-35).

15. Regarding claim 30, *Desai* discloses an outputting unit operable to output the password read by said reading unit to the communication terminal device (column 4, lines 32-67, “information exchange system and its storage system may be distributed across a plurality of devices”, column 5, lines 66 and 67, column 6, lines 1-25, column 9, lines 19-31, column 15, lines 27-44 and 55-67, column 16, lines 1-3, column 20, lines 36-67, column 21, lines 1-9 and column 22, lines 23-43).

16. Regarding claim 31, *Desai* discloses an application storing unit for storing therein a piece of application software that corresponds to the password (column 1, lines 26-51, column 2, lines 3-53, column 3, lines 42-67, column 4, lines 1-31, column 9, lines 1-18,

"registered user's profile data is kept private by the information exchange system 10 until the registered user 12 provides access to a view of the stored data", column 15, lines 27-44 and 55-67 and column 16, lines 1-3);

an application executing unit operable to execute the piece of application software, using the password read by said reading unit (column 1, lines 26-51, column 2, lines 3-53, column 3, lines 42-67, column 4, lines 1-31, column 9, lines 1-18, "registered user's profile data is kept private by the information exchange system 10 until the registered user 12 provides access to a view of the stored data", column 15, lines 27-44 and 55-67 and column 16, lines 1-3).

17. Regarding claim 32, Desai and Eldridge disclose a password recovery method to be used by a password recording medium that is portable and operable to re-supply a password to a user who has forgotten the password (*Desai* – column 2, lines 29-53, column 3, lines 42-62, column 8, lines 27-41, column 15, lines 27-67 and column 16, lines 1-3 and *Eldridge* – column 8, lines 63-67, column 9, lines 1-13 and 28-35 and column 11, lines 5-33, "diskette 142, CD-ROM 147"), the password recording medium comprising:

a public key storing unit for storing therein a public key that corresponds to a secret key belonging to a guarantor who guarantees legitimacy of the user (*Desai* – column 5, lines 24-39, column 12, lines 29-41 and 54-67, column 13, lines 1-8, column 15, lines 27-67, column 16, lines 1-3 and 34-42, column 17, lines 11-40 and column 21, lines 10-30 and *Eldridge* – Figures 3A, 3B, 5, 6B and 9, column 1, lines 66 and 67, column 2, lines 1-8, 31-47 and 64-67, column 3, lines 1-10, column 4, lines 62-67,

column 5, lines 1-24, "one type of encryption key suitable for use as secret parameter 302 is a RSA private encryption key", column 7, lines 19-48, column 8, lines 63-67 and column 9, lines 1-13 and 28-35);

a password storing unit for storing the password therein (*Desai* – Figure 11, column 2, lines 29-53, column 3, lines 42-62, column 5, lines 66 and 67, column 6, lines 1-25, column 9, lines 1-18, "registered user's profile data is kept private by the information exchange system 10 until the registered user 12 provides access to a view of the stored data", column 15, lines 27-44 and 55-67 and column 16, lines 1-3), the password recovery method comprising:

a receiving step of receiving a signed data set generated with use of the secret key (*Desai* – column 4, lines 32-67, "information exchange system and its storage system may be distributed across a plurality of devices", column 5, lines 66 and 67, column 6, lines 1-25, column 9, lines 19-31, column 15, lines 27-44 and 55-67, column 16, lines 1-3, column 20, lines 36-67, column 21, lines 1-9 and column 22, lines 23-43);

an authentication step of reading the public key from the public key storing unit and performing signature authentication using the read public key and the signed data set so as to judge if the received signed data set has been signed by the guarantor (*Desai* – Figures 11 and 17, column 2, lines 29-53, column 3, lines 42-62, column 5, lines 66 and 67, column 6, lines 1-25, column 9, lines 1-18, "registered user's profile data is kept private by the information exchange system 10 until the registered user 12 provides access to a view of the stored data", column 15, lines 27-44 and 55-67, column 16, lines 1-3 and column 18, lines 53-67 and *Eldridge* – Figures 3A, 3B, 5, 6B and 9, column 1,

lines 66 and 67, column 2, lines 1-8, 31-47 and 64-67, column 3, lines 1-10, column 4, lines 62-67, column 5, lines 1-24, "one type of encryption key suitable for use as secret parameter 302 is a RSA private encryption key", column 7, lines 19-48, column 8, lines 63-67 and column 9, lines 1-13 and 28-35);

a reading step of, when the authentication step judges that the signed data set has been signed by the guarantor, reading the password from the password storing unit (*Desai* – Figures 11 and 17, column 9, lines 1-18, "registered user's profile data is kept private by the information exchange system 10 until the registered user 12 provides access to a view of the stored data", column 18, lines 53-67, column 20, lines 36-67, column 21, lines 1-9 and column 22, lines 23-43 and *Eldridge* – Figures 3A, 3B, 5, 6B and 9, column 1, lines 66 and 67, column 2, lines 1-8, 31-47 and 64-67, column 3, lines 1-10, column 4, lines 62-67, column 5, lines 1-24, "one type of encryption key suitable for use as secret parameter 302 is a RSA private encryption key", column 7, lines 19-48, column 8, lines 63-67 and column 9, lines 1-13 and 28-35).

18. Regarding claim 33, *Desai* and *Eldridge* disclose a computer-readable storage medium on which a password recovery program is recorded for execution within a computer, the password recovery program being used by a password recording medium that is portable and operable to perform a password recovery method of re-supplying a password to a user who has forgotten the password (*Desai* – column 2, lines 29-53, column 3, lines 42-62, column 8, lines 27-41, column 15, lines 27-67 and column 16, lines 1-3),

the password recording medium comprising:

a public key storing unit for storing therein a public key that corresponds to a secret key belonging to a guarantor who guarantees legitimacy of the user (Desai – column 5, lines 24-39, column 12, lines 29-41 and 54-67, column 13, lines 1-8, column 15, lines 27-67, column 16, lines 1-3 and 34-42, column 17, lines 11-40 and column 21, lines 10-30 and *Eldridge* – Figures 3A, 3B, 5, 6B and 9, column 1, lines 66 and 67, column 2, lines 1-8, 31-47 and 64-67, column 3, lines 1-10, column 4, lines 62-67, column 5, lines 1-24, “one type of encryption key suitable for use as secret parameter 302 is a RSA private encryption key”, column 7, lines 19-48, column 8, lines 63-67 and column 9, lines 1-13 and 28-35);

a password storing unit for storing the password therein (*Desai* – Figure 11, column 2, lines 29-53, column 3, lines 42-62, column 5, lines 66 and 67, column 6, lines 1-25, column 9, lines 1-18, “registered user’s profile data is kept private by the information exchange system 10 until the registered user 12 provides access to a view of the stored data”, column 15, lines 27-44 and 55-67 and column 16, lines 1-3), the password recovery method comprising:

a receiving step of receiving a signed data set generated with use of the secret key (*Desai* – column 4, lines 32-67, “information exchange system and its storage system may be distributed across a plurality of devices”, column 5, lines 66 and 67, column 6, lines 1-25, column 9, lines 19-31, column 15, lines 27-44 and 55-67, column 16, lines 1-3, column 20, lines 36-67, column 21, lines 1-9 and column 22, lines 23-43);

an authentication step of reading the public key from the public key storing unit and performing signature authentication using the read public key and the signed data

set to judge whether the received signed data set has been signed by the guarantor (*Desai* – Figures 11 and 17, column 2, lines 29-53, column 3, lines 42-62, column 5, lines 66 and 67, column 6, lines 1-25, column 9, lines 1-18, “registered user’s profile data is kept private by the information exchange system 10 until the registered user 12 provides access to a view of the stored data”, column 15, lines 27-44 and 55-67, column 16, lines 1-3 and column 18, lines 53-67 and *Eldridge* – Figures 3A, 3B, 5, 6B and 9, column 1, lines 66 and 67, column 2, lines 1-8, 31-47 and 64-67, column 3, lines 1-10, column 4, lines 62-67, column 5, lines 1-24, “one type of encryption key suitable for use as secret parameter 302 is a RSA private encryption key”, column 7, lines 19-48, column 8, lines 63-67 and column 9, lines 1-13 and 28-35);

a reading step of, when the authentication step judges that the signed data set has been signed by the guarantor, reading the password from the password storing unit (*Desai* – Figures 11 and 17, column 9, lines 1-18, “registered user’s profile data is kept private by the information exchange system 10 until the registered user 12 provides access to a view of the stored data”, column 18, lines 53-67, column 20, lines 36-67, column 21, lines 1-9 and column 22, lines 23-43 and *Eldridge* – Figures 3A, 3B, 5, 6B and 9, column 1, lines 66 and 67, column 2, lines 1-8, 31-47 and 64-67, column 3, lines 1-10, column 4, lines 62-67, column 5, lines 1-24, “one type of encryption key suitable for use as secret parameter 302 is a RSA private encryption key”, column 7, lines 19-48, column 8, lines 63-67 and column 9, lines 1-13 and 28-35).

19. It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of *Eldridge* within the system and

method disclosed by Desai in order to provide "a removable media apparatus which contains both current and non-current information associated with a client process which may be used to update a secure server process with the most current data during the authentication process" (*Eldridge* – column 1, lines 59-63).

Response to Arguments

20. Applicant's arguments with respect to claims 19-33 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

21. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

22. The following United States Patents and Patent Application Publication are cited to further show the state of the art with respect to the recovery of data, such as:

United States Patent No. 7,083,090 to Zuili which is cited to show a remote and universal smartcard authentication and authorization device.

United States Patent No. 6,185,308 to Ando et al., which is cited to show a key recovery system.

United States Patent Application Publication No.20020034305 to Noyama et al., which is cited to show a method and system for issuing service and a method and system for providing service.

United States Patent No. 6,178,511 to Cohen et al., which is cited to show coordinating user target logons in a single sign-on (SSO) environment.

United States Patent No. 5,982,898 to Hsu et al., which is cited to show a certification process.

23. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeremiah Avery whose telephone number is (571) 272-8627. The examiner can normally be reached on Monday thru Friday 8:30am-5pm.

24. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

25. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JLA


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100